EHRs: Choice vs. Mandate

This document comprises research on EHRs, EHR vendors, Minnesota law, HIPAA, encryption, and internet security over the last three months. As one part of this inquiry, I've had frequent contact with two kind people at the Minnesota Department of Health (MDH), who have patiently answered my repeated questions. When I sent a draft of part of this document to them several days ago, however, which includes a proposed strategy for circumventing the mandate, things became colder. They would not confirm or disconfirm my statements; they requested that I not name my contacts there (I've wished to source everything I'm saying as specifically as possible, but I've granted their request); and they discouraged me from sending this document to you.

My inference about the MDH response is that they are understandably working under a mandate as well—to get EHRs accepted in Minnesota (see, for example, https://www.revisor.mn.gov/statutes/?id=62j.495, 62J.495, Subd. 2 (4)(c)). Further, I know they wish to be extremely careful about what they put in writing. I'm hopeful, however, that if there are indeed problems with a universal mandate to adopt EHRs, MDH will acknowledge them and work to find the best solutions.

In addition, I attended the 11/20/14 EHR seminar given by Trisha Stark, PhD, LP and Annie Schwain, MA, LADC, LAMFT as well as the 12/5/14 meeting of independent and small agency providers (by phone). Dr. Stark is a past president of the Minnesota Psychological Association (MPA) who sits on the e-Health Advisory Committee (which advises the Commissioner of Health on these matters). We owe her a great debt of gratitude for shouldering most of the work in studying and informing us about the EHR mandate. I understand she is offering another seminar on EHRs through MPA on January 9th. Dr. Stark, who has a more favorable opinion of EHRs than do I, also discouraged me from sending you this document.

Be that as it may, we all share the goal of forging the best path for health care in Minnesota. And I'm not opposed to the use of EHRs in all treatment contexts. But I currently believe—along with nearly every psychotherapist I've discussed the matter with—that a mandate that all psychotherapists use EHRs for all clients creates clear dangers for privacy, discussed below, and that both providers and clients should have the right to choose to avoid these dangers. I also believe that encroachments on the privacy of psychotherapy clients threaten the foundations of the psychotherapeutic process.

A fair amount of confusion and misinformation about EHRs is going around. In this statement, I've referenced everything I'm saying. Going forward, any assertion about EHRs should reference something written by the Minnesota Department of Health (MDH) or the relevant law itself including chapter and verse.

Obtaining answers to the really central questions I have about EHRs has been mind-numbingly difficult. Where I'm wrong, please enlighten me. If I'm quoting you, please correct me when I've misconstrued what you've said. This statement is being sent to all licensed psychologists in Minnesota as well as to the people at the Minnesota Department of Health, who I hope will also respond to this document. I'm also searching for ways to get this statement out to all the other licensed psychotherapists in Minnesota.

At the bottom line, I believe the security issues I will describe greatly skew the risk/benefit ratio of EHRs towards the extreme risk side.

Outline

EHR Basics

What is an EHR? "An electronic health record (EHR) is a digital version of a patient's paper chart. EHRs are real-time, patient-centered records that make information available instantly and securely to authorized users. . . . EHRs are built to share information with other health care providers and organizations – such as laboratories, specialists, medical imaging facilities, pharmacies, emergency facilities, and school and workplace clinics – so they contain information from all clinicians involved in a patient's care" (http://www.healthit.gov/providers-professionals/faqs/what-electronic-health-record-ehr).

An EHR records information about your evaluation, treatment planning, and session-to-session work with a client. This record resides on the internet and is thus potentially accessible in emergencies or by other health care professionals involved in a patient's treatment. At least part of it is accessible by a client. It is intended to improve communication between all health care professionals, helping them obtain a fuller, legible picture of a patient's health concerns.

EHRs appear to be particularly helpful to physicians, making it possible to reduce costs associated with storage, retrieval and transcription of patient files; obtain lab results rapidly; prevent duplication of services and diagnostic tests; avoid harmful medication interactions; communicate prescriptions legibly, and speed billing, among many other things. All of a patient's health information is available in one place, facilitating decision making about diagnosis and treatment. EHRs also allow tracking health care across large groups of patients. The best statement I've found regarding the purpose and value of EHRs is at http://www.healthit.gov/providers-professionals/benefits-electronic-health-records-ehrs.

EHRs can also be a convenience to patients. If you switch ophthalmologists or ENTs, it's nice to have your records automatically follow you.

Interoperability. EHRs involve your client data being stored in the cloud, potentially available to other health care providers on the internet. The "interoperability" requirement for EHRs stipulates that required data can be exchanged "across systems and organizations . . . using standards for exchange and by connecting to a State-Certified Health Information Exchange Service Provider" (p. 2, http://www.health.state.mn.us/e-health/hitimp/2015mandateguidance.pdf). That is, the data on your EHR must be automatically readable and storable into someone else's EHR.

You apparently don't have to have an EHR by January 1st (per 11/20/14 Stark/Schwain seminar; I did not confirm this with MDH). Most vendors aren't up to speed on psychotherapy EHRs yet. Dr. Stark stated that at this point, we should write a paragraph on our next steps regarding implementing EHRs but that we may not be expected to have one in place for one or two years. Further, the Minnesota Department of Health (MDH) has stated that for now, there is no penalty for not having an EHR (p. 1,

http://www.health.state.mn.us/e-health/hitimp/2015mandateguidance.pdf). The fact that this initiative is well behind schedule means that there is time to work to modify the law before it takes full effect.

The federal government is not mandating that psychotherapists use EHRs. In fact, it is not actually mandating EHR use for anyone. Rather, it is penalizing Medicare/Medicaid providers who do not adopt EHRs by reducing compensation 1% per year (http://www.healthit.gov/providers-professionals/faqs/are-there-penalties-providers-who-don%E2%80%9A%C3%84%C3%B4t-switch-electronic-health-record). Minnesota's mandate appears to be unique in the country—in being a mandate, in requiring all providers to comply, and in applying across compensation types—that is, whether a provider receives Medicare/Medicaid, private insurance, or out-of-pocket compensation (more on this under "To Whom Does the Mandate Apply?" below).

The Minnesota legislature, though well intentioned, has gone far beyond the "nudge" principle that has usefully informed much government strategy lately and that essentially involves small pushes in desired directions that still allow choice (http://www.apa.org/monitor/2014/12/cover-coaxing.aspx) to one that is purely authoritarian.

The best and possibly only way for smaller practices to obtain an EHR solution is through web portal products, from which one downloads client files as needed, updates them, then stores them in the cloud. This was stated in the 11/20/14 seminar. Client data are stored via the internet and backed up by your EHR vendor. Any needed programming updates are handled automatically by the vendor. Ronald Manke of NJ-HITECH was paraphrased as saying that "most small practices lack the technical expertise to deal with the manifold challenges of operating an EHR system onsite" (http://www.ihealthbeat.org/insight/2013/physicians-divided-on-cloudbased-ehrs). Apparently onsite solutions would also be prohibitively expensive for a small provider.

But if you don't have an onsite solution, one added risk is that your client files are no longer in your possession. According to hl7standards.com: "Full Circle Health Care in Maine purchased an EHR from HealthPort in 2010. Originally the maintenance fees were $300 a month. A few months later CompuGroup Medical purchased HealthPort and increased the maintenance fees to $2,000 a month. The practice protested the price increase and claimed CompuGroup failed to deliver hardware upgrades that had been paid for. The parties spent several months arguing and for 10 months the practice did not pay its maintenance bills. Finally in July, CompuGroup shut off the practice's access to its medical records" (http://www.hl7standards.com/blog/2014/10/21/ehrs-first-do-no-harm/).

Other problems may arise. What happens to your scheduled session and pre-session review when your internet service provider is having a bad day or hour? How much will costs increase over time once a vendor has you as a customer? If you decide you want to

switch vendors, transferring all your client files from one EHR format to another, how difficult and expensive will this be three years down the road? Possibly very easy because of "interoperability"? Possibly not. There are numerous possible problems here, though many solvable.

It may or may not be possible to keep working psychotherapy notes off the EHR, for example in handwritten form. To review: "psychotherapy notes" are defined as "notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record" (p. 76, http://www.hhs.gov/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf).

Dr. Stark has stated that it will be possible to keep psychotherapy notes off the EHR (11/20/14 seminar). I can't find anything in the law that contradicts this, although I can't find a clear written statement confirming it, either in law or from the MDH. It would be inconvenient to keep notes in two places, but doing so may be a measure of privacy protection. An individual at MDH has mentioned to me informally that some of the national EHR advocates are pushing to have everything on the EHR. This may therefore be a slippery slope.

What information must go on an EHR? This question is apparently still being decided. HIPAA defines the following information as separate from "psychotherapy notes": "*Psychotherapy notes* excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: Diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date" (p.76, http://www.hhs.gov/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf). Presumably this information would go on the EHR.

The 11/20/14 seminar handout (p.8) lists the following under "What should be in the Mental Health Information Set?": evaluations, assessments, cognitive impairments, trauma history, commitment status, danger to self or others, substance abuse, contact information for all providers, medication list, psychiatric advance directive, diagnosis, procedure codes, treatment plans, and problem lists.

Some psychotherapy clinics in the Twin Cities have already adopted EHRs. A colleague who works at one has listed for me the information their EHRs include (at this writing, he hadn't yet reached the CEO to ask permission to name the clinic):

- summary review—diagnosis, test results (clients take a PHQ-9 at each visit)
- mental health symptom checklist: 15 possible symptoms include sleep disturbance, appetite, ruminations, compulsions, etc.

- mental status exam: affect, appearance, attention, attitude, mood, insight, judgment, orientation, thought process (circumstantial, disassociation, etc.)
- functional impairment: problems or challenges in vocation, self-care, finances, housing
- risk factors for chemical health: suicidal ideation (thoughts, attempts); homicidal ideation, self harm, tobacco use, substance abuse
- progress notes
- visit summary

The 12/5/14 meeting for independent and small agency providers was concerned with what limited information might go on a Continuity of Care Document, although not with what information would go on the EHR itself. This meeting—facilitated by Dr. Stark and James Dungan-Seaver, IT manager, Hamm Clinic and attended by 43 psychotherapists—was intended to "reach an agreement among those present on what specific client mental health information should be available for health information exchange" (10.22.14 circular announcing the meeting).

Dr. Stark stated to me in a 12.12.14 email that the information under discussion was a smaller part of the total information that would be on the EHR. An MDH contact explained to me in a 12.12.14 email that the meeting was about "a limited data set of information that BH [behavioral health] providers in Minnesota would include in a BH CCD-A [Continuity of Care Document Architecture], should that be developed." A CCD, containing information extracted from the EHR, summarizes important healthcare information for communication with other providers. It is useful, for example, in emergency situations as well as future treatment. The meeting facilitators planned to submit a memorandum summarizing the meeting results to the eHealth Advisory Committee, which makes recommendations to the Minnesota Commissioner of Health regarding e-health matters.

A common argument for EHRs is that in certain situations, psychological information might be useful to ER personnel. The preparatory materials for the 12/5/14 meeting offered an "Emergency Room Scenario" for possible discussion and stated: "The most compelling case in favor of sharing health information invokes an emergency room scenario."

The scenario described a single woman brought by ambulance to an ER who then had a heart attack. Coming out of surgery or out of a post-surgical medically induced coma, would ER providers find it useful to have mental health information such as pre-crisis diagnoses and functional/cognitive status? My discussions with a neurologist and a cardiology nurse practitioner suggested that the main post-surgery concerns regarding mental status would be to bring the patient out of delirium if present. Rehab would later find it useful to know pre-status cognitive/functional status, but this information would not be needed rapidly. And surely if cognitive/functional status were significantly compromised pre-crisis—i.e. useful as benchmarks in a rehab setting—they would be

part of any medical EHR. I'm unaware of any imminent need for information from a psychologist in this example unless he or she prescribed medication.

There may be better examples of a true need for psychological information in emergency situations. But possible risks associated with absence of psychological information on EHRs in rare emergency cases must be weighed against risks to the privacy of *all* psychotherapy clients, discussed below.

Including psychotherapy information on the EHR is of questionable benefit to a client relative to privacy concerns. In my experience and that of other experienced psychotherapists with whom I've spoken, psychotherapy information on EHRs is typically of questionable interest to other health care providers—unless one is working within an integrated care setting such as pain, rehabilitation, primary care, or multidisciplinary psychiatric clinics. In addition, adult clients are capable of remembering and when necessary bringing any useful medical information to psychotherapy sessions (they will in fact be able to access much of it themselves via EHRs). Again, the occasional added benefit of being able to view such information on the EHR ourselves is greatly outweighed, in my opinion, by sacrifices to the security of a client's private information.

When will the information on a client's EHR be accessible to other health care providers without client consent? In my reading, Minnesota law states that patient information is available without consent only in an emergency (2007 Minnesota Session Laws, Chapter 147, Article 10, 144.293 https://www.revisor.mn.gov/laws/?id=147&year=2007).

To Whom Does the Mandate Apply?

It appears that the Minnesota Department of Health (MDH) considers that the mandate applies to all, even those who have a fee-for-service practice, only do life coaching, etc. The law mandates that all "health care providers" have EHRs, according to the MDH's *Guidance for Understanding the Minnesota 2015 Interoperable EHR Mandate* (p. 4) (http://www.health.state.mn.us/e-health/hitimp/2015mandateguidance.pdf). As explained there, the law itself stipulates that "health care provider" includes an individual who provides health care services "for a fee" and is "eligible for reimbursement under the medical assistance program." The law goes on to widen this definition:

> "For a fee" includes traditional fee-for-service arrangements, capitation arrangements, and any other arrangement in which a provider receives compensation for providing health care services or has the authority to directly bill a group purchaser, health carrier, or individual for providing health care services. For purposes of this subdivision, "eligible for reimbursement under the medical assistance program" means that the provider's services would be reimbursed by the medical assistance program if the services were provided to medical assistance enrollees and the provider sought reimbursement, or that the services would be eligible for reimbursement under medical assistance except that those services are characterized as experimental, cosmetic, or voluntary [underline mine].

The (awkward) phrasing of the last clause, and especially the word *voluntary*, greatly widens the definition of health care provider—essentially including everyone—at least as stated by an individual at MDH in a 10.27.14 phone contact.

The footnote on p. 3 of MDH's *Guidance* may widen the definition of health care provider still further, even to those who do not charge for services, although the phrasing may have other interpretations: "MDH understands the §62J.03 portion of the 2015 Interoperable EHR Mandate to include any health care provider who provides a service that could be reimbursed by Medical Assistance or MinnesotaCare, whether or not the provider accepts these patients or accepts payment for the service."

The wide definitional sweep is curious. If EHRs are about reducing costs, why would life coaches and others who do work outside the medical model be required to have EHRs, given that no government agency or health insurance provider pays for such work? Perhaps it is thought that information from their work would inform medical care or vice versa, but this is certainly a stretch.

Interestingly, the definition of "health care provider" was created in 1993 (1993 MN Session Laws, Chapter 345, Article 6, Section 1, Subd 8) (https://www.revisor.mn.gov/laws/?id=345&year=1993&type=0) and the mandate that all "health care providers" must have EHRs was created in 2007 (MN Session Laws, Chapter 147, Article 15, Section 2, Subdivision 1 (https://www.revisor.mn.gov/laws/?id=147&year=2007&type=0). In all this complexity,

were legislators able to appreciate the full meaning of their mandate? (And could legislators in 2007 anticipate the security problems on the 2014 internet?)

What about clients who pay out of pocket? It was stated at the 11/20/14 seminar that the one exception to the mandate is for clients who pay out of pocket, who may keep their information off of an EHR. What does the law say? The only HIPAA reference I can find regarding out-of-pocket payments states that individuals who pay this way may deny their provider permission to share information with the individual's health plan. Apparently the information could still be on an EHR but would not be communicated to the health plan. This is in HITECH Act Section 13405(a) (see http://www.hipaasurvivalguide.com/hitech-act-13405.php). I've found nothing in writing from MDH suggesting that clients who pay out of pocket are exempt from having an EHR—in fact just the opposite as noted in the section just above.

By the way, a participant at the 11/20/14 seminar reported that an attorney had stated that clients with insurance cannot opt to pay out of pocket and that a provider allowing this would be seen as committing fraud by the health plan. This appears to be untrue. As stated in the above paragraph, HIPAA gives permission for just such a situation. Clients paying out of pocket can keep their treatment hidden from their health plans, and providers must respect their wishes.

I believe it was also stated at the 11/20/14 seminar that if clients choose not to have a psychological EHR, they cannot have a medical EHR either. This also appears to be untrue. This assertion may have to do with Minnesota law concerning the record locator service, an online index that points a provider to a patient's health records (2007 Minnesota Session Laws, Chapter 147, Article 10, 144.291, Subd. 2(i) at https://www.revisor.mn.gov/laws/?id=147&year=2007). But this law states that patients may exclude all their information from the record locator service or just have "a specific provider contact excluded" (144.293, Subd. 8(d)). In any case, excluding information from a record locator service isn't the same as choosing not to have an EHR—one might still have an EHR. Finally, in a 12/5/14 phone conversation, an MDH contact also confirmed that nothing prevents a patient from having a medical EHR.

If all of the information and inferences above are true, it's possible that all psychotherapists must maintain an EHR for all clients, but if there were indeed exceptions to this statement, their clients could still have medical EHRs.

Is there a way around the mandate? An excerpt follows from my 12/8/14 email to an MDH contact [for the HIPAA Privacy Rule 164.522 alluded to in the email, see http://www.hipaasurvivalguide.com/hipaa-regulations/164-522.php]:

> I see that an individual [client] does have the right to request information not be disclosed. The provider may but does not have to agree to this restriction . . . . This is in the [HIPAA] Privacy Rule, 164.522.

> One way—the simplest way—to ensure that this information is safely kept undisclosed would be to refrain from putting it on an EHR in the first place. I can't find anything in law that states that: 1) an individual cannot ask for all information to be kept off an EHR or 2) a provider may not agree to such a request, though a provider could certainly refuse. If such a request were agreed to, informed consent would naturally be given—i.e. the provider would discuss costs/benefits of this decision.
>
> It seems to me that such a request would fall within the larger right of an individual to consent or not to any medical or psychological treatment as well as the right to determine one's own level of privacy. An obvious example might be a famous person, but any person should certainly have choice in this matter.
>
> I'm curious if there is anything in law that contradicts what I'm saying?

My MDH contact replied that my questions required legal review and that upcoming MDH workgroups may consider such questions. I hope they will do so. I respect their need to be precisely careful about what is communicated. Be that as it may, shouldn't *any* client, paying out of pocket or not, have the right to keep his or her private information off an EHR? And shouldn't any provider have the right to grant such a request? If so, when a provider refused such a request, the client could choose to look for help elsewhere. What health plans may or may not eventually have the right to say about this issue may be another question.

Informed consent. One of the great ethical precepts, written into our board rules, is informed consent. If we give thorough informed consent about the security dangers of EHRs (covered below), it seems to me that many if not most psychotherapy clients would refuse to grant permission to use them. In some treatment contexts, however, such as integrated care in which a psychologist works with multiple health care disciplines, the risk/benefit ratio for EHRs rebalances. A psychotherapist working in such contexts might conceivably refuse to see a client who refuses to have an EHR or simply be unable to conveniently grant a request to have documentation kept elsewhere—leaving it up to the client to decide whether to proceed. Working in private practice, I would like to refuse to see clients who wish to have a psychotherapy EHR (pending confirmation of legality by MDH or legal consultation) because the security problems I see with them are so great.

On 12.16.14, I sent an earlier draft of this whole section, "To Whom Does the Mandate Apply?" to my contacts at MDH to examine in order to confirm or disconfirm my quotes of them and ascertain I wasn't passing on misinformation. Unfortunately, they would not do so, but in any case assertions made about EHRs should be grounded in more formal, written statements from MDH or in the law itself.

Privacy and Security: General Concerns

Privacy vs. security: definitions.

- "Security or Security measures encompass all of the administrative, physical, and technical safeguards in an information system" (http://www.hipaasurvivalguide.com/hipaa-regulations/164-304.php)

- Although HIPAA has a Privacy Rule, I couldn't find a HIPAA definition of privacy. For our purposes, I think we can say, "The ability to choose to keep personal information from the view of others."

Strong evidence exists, outlined below, that the security of information in the cloud is very uncertain. The idea that security there is anything close to that of your locked file cabinet appears deeply flawed. Marla Durben Hirsch of FierceEMR has warned that consumers are "going to wake up and realize how vulnerable EHRs can be to privacy and security breaches. It's unfortunately much easier for electronic patient records to be lost, stolen or hacked than paper records, and when a breach occurs, it usually affects many more records at a time. It's also harder to protect electronic patient records when they're stored or accessible in the cloud or via third-party health information exchanges, where the provider has less control over what safeguards are being taken with his/her patients' data" (http://www.fierceemr.com/story/patients-withholding-info-ehrs-has-far-reaching-consequences/2014-07-30).

Psychotherapy requires not just privacy but the *feeling* of privacy, which is why we have strict laws and board rules about it. To engage in psychotherapy freely and openly, clients must feel completely safe regarding their privacy. We give them informed consent so they have control over their privacy. We erect sound barriers. We warn them about the dangers of unencrypted email. The idea of personal information floating in the cloud threatens the sanctuary of psychotherapy.

A September, 2013 Pew Research Center survey found that "Sixty-six percent of U.S. Internet users polled believe current laws aren't good enough to protect people's privacy online" (http://www.bloomberg.com/news/2013-09-06/nsa-code-cracking-puts-google-yahoo-security-under-fire.html). How much will this level of insecurity bleed into sensitivity about EHRs and therefore into the psychotherapeutic relationship itself?

How will clients feel about psychological diagnoses or even their contact with a psychotherapist being potentially discoverable on the internet, not to mention a wealth of other psychological information? Many clients, in my experience, are uncomfortable with me even contacting their physicians. (This concern is also described in Richards, M.M., Electronic medical records: Confidentiality issues in the time of HIPAA, *Professional Psychology: Research and Practice*, 2009, 550-56.)

Psychotherapy information cannot be treated like medical information. People are understandably sensitive about their medical privacy (see next section), but far more so about their psychotherapeutic privacy. Calling us all "health care providers" and applying the same rules across the board is problematic. There is currently a push to include psychologists in Medicare's "physician" definition, which is great in some respects, but in practice we're different from each other. Indeed, psychotherapists have generally had greater concerns about privacy and confidentiality long before the advent of HIPAA. Privacy is foundational to the work of psychotherapy, which is built on trust.

Evidence that EHRs appear to affect patient self-disclosure. A July 2014 study in the *Journal of the American Medical Informatics Association* "suggests that patients are withholding information from their health providers because of privacy and security concerns related to electronic health records. . . . The researchers analyzed a nationally representative sample from the 2012 Health Information National Trends Survey . . . and found that about one in eight patients—close to 13 percent—have withheld information from a physician for privacy or security reasons. A multivariate analysis of the results found a correlation between patients withholding information and their physician using an EHR during the patient encounter" (http://www.clinical-innovation.com/topics/ehr-emr/do-ehr-privacy-and-security-risks-affect-patient-disclosure). How much more sensitive about psychological information will people be? Before EHRs are mandated, shouldn't their use be thoroughly researched and shown not to influence client comfort and disclosure?

Medical identity information is a prime target for theft, according to a February 2014 report by Kaiser Health News (http://kaiserhealthnews.org/news/rise-of-indentity-theft/). The report stated that medical information is useful for numerous reasons. As one example, "a Massachusetts psychiatrist created false diagnoses of drug addiction and severe depression for people who were not his patients" to submit false insurance claims. Medical information is useful in illegally procuring drugs as well as health care including surgery. In 2013, "medical-related identity theft accounted for 43% of all identity thefts reported in the United States."

The Identity Theft Resource Center's description of the November 2014 data-breach at Sony stated: "The Sony breach exposes a new threat realm that includes stealing and exposing health-care information, employee e-mails and project e-mails involving clients, partners and other employees. Can you imagine private e-mails from your employer, health provider, banker, social media or child's school about your salary, medical records, credit score, child's grades, personal or business relationships going public for everyone to read and see?" (http://www.idtheftcenter.org/Data-Breaches/is-sony-data-breach-a-sign-of-things-to-come-in-2015.html)

But breaches of medical records are hardly new. Since 2009, 31.7 million medical records have been breached in a variety of ways, including hacking/information technology incidents (98 incidents, millions of records), improper disposal, loss, theft,

and unauthorized access/disclosure (http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html). The president of the American Medical Association Board, Robert Wah, has stated: (http://www.benefitspro.com/2014/07/14/ehr-security-breaches-on-the-rise?page=2):

> "What I think it's going to lead to, if it hasn't already, is an arms race between the criminal element and the people trying to protect health data. 'They're seeking health records because they can do huge financial, fraudulent damage, more so than they can with a credit card number or Social Security number.'"

In April, 2014, "the FBI warned healthcare organizations that their electronic data protection systems were lax compared with other sectors. 'Health data is far more valuable to hackers on the black market than credit card numbers because it tends to contain details that can be used to access bank accounts or obtain prescriptions for controlled substances'" (http://www.policymed.com/2014/08/electronic-health-records-update-as-adoption-of-ehrs-increases-so-do-privacy-and-data-security-conce.html#sthash.8T0RTkrf.dpuf).

How EHRs Protect Privacy

Encryption. Health Information Technology Standards mandate that electronically transmitted client information must be encrypted at a certain level (HIT Standards 170.210, see http://www.hipaasurvivalguide.com/hit-subchapter-d/hit-170-210.php). Your EHR vendor would be responsible for meeting this standard, and you would be trusting the vendor to do so. With EHRs, we must put our trust in others regarding what standards are deemed safe as well as their careful adherence to those standards. Control no longer in our hands.

Currently, encryption at levels Health and Human Services recommends (though does not enforce--see http://experts.niu.edu/law/organizations/law_review/pdfs/full_issues/30_3/Wafa.pdf) may be unbreakable (http://www.computerworld.com/article/2550008/security0/the-clock-is-ticking-for-encryption.html).

On the other hand, the Edward Snowden documents revealed that the National Security Agency has used its leverage with numerous companies to "insert vulnerabilities into Internet security products" (http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?pagewanted=4&_r=3&hp). Ed Black, president of a computer trade group, has stated: "By secretly embedding weaknesses into encryption systems in order to create a 'back door' for surveillance access, the NSA creates a road map for similar cyber-incursions by others with less noble intentions" (http://www.bloomberg.com/news/2013-09-06/nsa-code-cracking-puts-google-yahoo-security-under-fire.html).

The New York Times article linked in the above paragraph also stated: "How keys are acquired is shrouded in secrecy, but independent cryptographers say many are probably collected by hacking into companies' computer servers, where they are stored." [Apple dictionary: a server is "a computer that provides services (such as file services, mail services, or web services) to other computers or network devices." EHR vendors will provide their services via servers.]

The Snowden documents also revealed that the NSA is building a quantum computer "that could break nearly every kind of encryption used to protect banking, medical, business and government records … part of a $79.9 million research program titled 'Penetrating Hard Targets'" (http://www.washingtonpost.com/world/national-security/nsa-seeks-to-build-quantum-computer-that-could-crack-most-types-of-encryption/2014/01/02/8fff297e-7195-11e3-8def-a33011492df2_story.html). If the NSA is doing so, unquestionably other entities around the world, both government and criminal, are doing so as well. The internet is like the bar in Star Wars. What dangers lurk there are difficult to know and difficult to predict.

Audit logs. In addition to encryption, Minnesota law provides a sort of back door safeguard called an "audit log," which records the identity and date of a provider accessing patient information (144.293, Subd. 8(b)). One can presumably then run a report to see who has accessed the EHR. Further, patient compensatory damages are provided for when a provider accesses this information in a non-emergency situation without permission (144.298, Subd. 2, https://www.revisor.mn.gov/laws/?id=147&year=2007).

Data Segmentation. Technology is being developed for data segmentation, by which specific parts of a client's EHR can be hidden from providers with whom the patient chooses not to share that information (http://www.ihealthbeat.org/articles/2014/6/5/samhsa-to-hold-public-meeting-on-patient-consent-rules-and-ehrs). I'm unclear how this technology fits with Minnesota law or what difference it would make, given that all information would presumably still be available in an emergency and none otherwise without consent.

Annual updates of security procedures. Another strategy for keeping health care information safe, described in the HITECH Act, is a mandate that the Secretary of Health and Human Services "annually issue guidance on the most effective and appropriate technical safeguards" to meet security provisions (http://www.hipaasurvivalguide.com/hitech-act-13401.php). This plan implicitly acknowledges that security strategies will not remain stably effective. Hackers and criminals continue to improve their techniques. What happens in the gap between hacker advances and the annual update?

Problems with EHR Security

These are complex issues. There may or may not be errors in some of what I've written above or below. I'm eager for feedback from others, including you and I hope in time MDH. But whether or not there are a few errors here, a clear picture emerges about the security vulnerabilities of EHRs.

I've studied EHRs for three months. If I'm unsure about some of these issues, you're likely to be as well. The use of EHRs takes client security largely out of our hands and understanding. With EHRs, we cannot assure clients that we are anything close to fully responsible for the privacy of what they tell us.

Potential Access by Many

First, balanced against the safeguards outlined above are the numberless entrances into the online EHR universe. There are, for example, 9000 Urgent Care Centers in the United States (http://www.beckershospitalreview.com/lists/25-things-to-know-about-urgent-care.html). In my understanding, several physicians and perhaps other personnel at each ER will have access to EHRs in the cloud. In addition, all Minnesota health care providers (and eventually all medical providers, chiropractors, etc., etc. in Minnesota? in the United States?) will have access to EHRs.

Further, it's not just health care providers who will have access to EHRs. All EHR vendors will have access to them. That is, at least some vendor personnel will obviously have access to the encryption key they use to decrypt their EHRs. I'm unclear how they will handle passwords, but providers will lose their passwords and need to retrieve them. Where will they be stored, and which vendor personnel would potentially have access to them? I asked two vendors about their plans for limiting access to encryption keys and passwords but did not receive a response.

So the first problem is that so many people have access. True, any access to an EHR would be electronically recorded, and penalties would exist for wrongful access. But who would be responsible for committing time and financial resources to monitoring such incursions? Would access reports be sent to providers automatically, and how would they know access was legitimate or not without time-intensive work? Would health care providers, who are overworked, have the time to check such things? The four-year breach of the electronic medical records of the five-hospital Riverside Health System in Virginia, announced in December 2013, was discovered via a "random company audit" (http://www.healthcareitnews.com/news/four-year-ehr-breach-raises-eyebrows).

Al Saikali, a partner in a Miami data security company, has said, "With so many hands on a medical record and the copies of the medical record, there are plenty of opportunities for unauthorized access or acquisition of those records" (http://www.benefitspro.com/2014/07/14/ehr-security-breaches-on-the-rise?page=2). Wendy Franklin, Director of Development and Human Relations at North County

Hospital in Newport, VT, has stated that although the hospital encrypts most of its health records and audits access to them, "the hospital largely has to rely on the honor system" http://kaiserhealthnews.org/news/rise-of-indentity-theft/.

Of course, access reports merely note when the horse is out of the barn. They are retrospective. And what about health care or vendor personnel stealing passwords or encryption keys, leaving for another job, and selling them on the black market a few months later?

I wouldn't worry so much in these directions if it were not for the countless, faceless individuals, including criminal elements, who will have the potential to access EHRs, who together increase the chances of breaches far above the locked file cabinet. This fact alone raises legitimate questions about the wisdom of imposing a strict mandate for EHR adoption.

Stolen passwords

Employees are not the only people who can engage in password theft. As one example, in August 2014, the *New York Times* reported that Russian hackers had stolen 1.2 billion user name and password combinations (http://www.nytimes.com/2014/08/06/technology/russian-gang-said-to-amass-more-than-a-billion-stolen-internet-credentials.html?_r=0). Encryption won't protect security if the password and username to your EHR account are stolen.

Any health care professional is vulnerable to password loss. Some say, "Well, there are risks with any security solution." But when someone steals the key to your file cabinet, only your clients are placed at risk. When someone steals your password to the EHR universe, everyone's clients are placed at risk.

Again, in addition to health care professionals, vendors and systems administrators will have potential access to EHRs, which opens the door to client files wider. A parallel is the November 2014 Sony breach, which occurred because hackers were able to steal "the computer credentials of a Sony systems administrator to get access to Sony's computer system" (e.g., http://ktla.com/2014/12/18/hackers-stole-credentials-of-sony-systems-administrator-report/).

Malware

Malware can do several things. "When the device is in use and the user has been authenticated to the storage encryption solution, malware could access decrypted files and transfer copies of them to external hosts or extract sensitive information from them. Other examples are an attacker disabling or reconfiguring storage encryption . . . [and] malware installing a keylogger that captures passwords used for storage encryption authentication" (http://csrc.nist.gov/publications/nistpubs/800-111/SP800-111.pdf).

So when you are accessing a client EHR on your computer, it is decrypted, and malware could take a snapshot of the information and send it over the internet to another site. And a malware keylogger can steal your password, allowing access to all your client EHRs as well as to the EHRs of others.

According to the 11.30.14 *60 Minutes* feature on malware, "Swiping Your Card" (http://www.cbsnews.com/news/swiping-your-credit-card-and-hacking-and-cybercrime/):

- "The number of reported illegal intrusions into the computer systems of U.S. companies is at a record high this year and climbing."
- "2014 is becoming known as the 'year of the data breach.'"
- The CEO of cybersecurity company FireEye, Dave DeWalt, stated: "Nearly every company is vulnerable" and "Ninety-seven percent of all companies are getting breached."
- The Target breach "started when criminals stole the username and password from one of Target's vendors -- a Pennsylvania heating and air conditioning company. The credentials got them into Target's network without attracting attention. Once inside they easily spread to thousands of checkout terminals in nearly every store. The hackers then installed malicious software, or malware, to record card swipes."
- DeWalt also stated: "On average the breaches from the time of infection, from when the bad guys get in to the time they are discovered, is a whopping 229 days."

But malware can remain hidden much longer. A version called Regin, which can "grab passwords, monitor network traffic and gather information from the computer's memory," had been operating on and off since 2008 until Symantec reported its existence on November 23, 2014. Versions of it may still be operating (http://bits.blogs.nytimes.com/2014/11/24/symantec-discovers-spy-code-lurking-on-computer-networks/?mabReward=RI%3A7&action=click&pgtype=Homepage&region=CColumn&module=Recommendation&src=rechp&WT.nav=RecEngine&_r=0). "Undeniably a spy tool," Regin has been used to gather information from numerous entities, including "academic researchers, individual and small businesses." Regin is now known, at least some versions of it. It is, of course, impossible to know what malware remains unknown or what new iterations of malware may be developed in the future.

How does malware get installed in a computer? In the *New York Times* article linked in the above paragraph, Symantec was quoted as stating that in one case, Regin "directed victims to spoofed versions of popular websites, then downloaded malware onto their machines." But a wide variety of methods exists. The IT department at Cornell states (http://www.it.cornell.edu/security/safety/malware/):

> Malicious software, such as viruses, worms, and Trojan horses, collectively known as malware, can end up on your computer via email attachments and drive-by downloads. It can sneak in when you download free software, especially free

> antivirus software. It lurks in seemingly innocuous ads, and takes advantage of vulnerabilities in peer-to-peer (computer networking) programs.
>
> There is really no guaranteed solution to prevent malware from invading your computer, especially since criminals spend a lot of time keeping ahead of the curve to find new and innovative ways to break down your computer's security defenses.

It's even conceivable that malware could be installed on your computer by a vendor, knowingly or unknowingly. A reliable way to prevent malware infections might be to stay off the internet, never install new software, and never allow other people access to your computer.

According to a 12.11.14 *New York Times* article, both Windows—which updates itself monthly with security patches—and yes, even OS X are vulnerable to malware (http://www.nytimes.com/2014/12/11/technology/personaltech/keeping-up-with-windows-update.html?mabReward=RI%3A6&action=click&pgtype=Homepage&region=CColumn&module=Recommendation&src=rechp&WT.nav=RecEngine&_r=0).

Security patches and antivirus updates are critical. Prior to the appearance of each corrective update, however, risk to client privacy would exist.

"As secure as online banking"

Claims have been made that "cloud-based EHRs are as secure as online banking" (http://www.ihealthbeat.org/insight/2013/physicians-divided-on-cloudbased-ehrs), and that "web-based EHR systems achieve HIPAA compliance through data centers with bank level security" (http://www.poweryourpractice.com/practice-management/5-advantages-of-a-cloud-based-ehr-for-small-practices/).

But DeWalt in the *60 Minutes* feature cited above stated: "Even the strongest banks in the world—banks like JPMorgan ... can't spend enough money or hire enough people to solve this problem." JPMorgan's network was hacked last summer, which took the bank more than two months to discover (http://dealbook.nytimes.com/2014/11/06/another-security-fix-made-to-jpmorgan-chase-corporate-challenge-charity-race-website/?mabReward=RI%3A8&action=click&pgtype=Homepage&region=CColumn&module=Recommendation&src=rechp&WT.nav=RecEngine).
In this breach, "hackers may have accessed the secure information of approximately 83 million of its accounts" (http://www.idtheftcenter.org/Data-Breaches/jpmorgan-confirms-data-breach-affecting-83million.html).

"The year of the data breach"

"The year of the data breach," in the words of the *60 Minutes* feature discussed above, has seen the heartbleed bug and well-publicized breaches at Target, Michaels, PF Changs, the White House, Home Depot, Forbes, the United States Postal Service, and Sony. But the problem is immeasurably more extensive. A recent Price Waterhouse (PwC) survey of security breaches found that "the total number of security incidents detected showed an increase of 48% over 2013," totaling 42.8 million (http://www.pwc.com/gx/en/consulting-services/information-security-survey/index.jhtml).

Last year was no slouch either. According to the IBM security division, the average American company experienced 16,856 attacks in 2013 (Grossman, L, The Code War, TIME, 7.21.14, p.25).

HHS's prescription for "secured PHI" isn't reassuring

HHS requires only breaches of unsecured protected health information to be reported (p. 42741, column 1, http://www.gpo.gov/fdsys/pkg/FR-2009-08-24/pdf/E9-20169.pdf). One might think, then, that everything will be fine if one follows closely the HHS rules for securing data, such as encryption.

But the definition of "unsecured PHI" appears to have a retrospective back door. That is, client data that once would be defined as secured becomes defined as unsecured if it is breached. Specifically, it's "unsecured" if means haven't been used to "render protected health information unusable, unreadable, or indecipherable to unauthorized individuals" (p. 42741, column 1, http://www.gpo.gov/fdsys/pkg/FR-2009-08-24/pdf/E9-20169.pdf). And to meet the "unusable, unreadable, or indecipherable" criterion, it must be encrypted AND "the confidential process or key that might enable decryption has not been breached" (p. 42742, column 3). Bottom line: if it's been breached, encrypted or not, it's not "secured" any more.

According to some of the information discussed earlier, such breaches might occur via employees, keystroke-logging malware, or hacking into companies' computer servers. Inspecting the HHS's wall of shame (http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html), I wasn't able to determine which breaches involved PHI that had been encrypted yet breached via password or encryption key theft.

Breaches of personal information appear to be increasing

- *New York Times*, 8/5/14: "There is worry among some in the security community that keeping personal information out of the hands of thieves is increasingly a losing battle. . . . For all the new security mousetraps, data security breaches have

only gotten larger, more frequent and more costly" (http://www.nytimes.com/2014/08/06/technology/russian-gang-said-to-amass-more-than-a-billion-stolen-internet-credentials.html?_r=0).

- Lillian Ablon of the Rand Corporation was quoted in the same article: "The ability to attack is certainly outpacing the ability to defend."
- And the *60 Minutes* feature quoted above: "The number of reported illegal intrusions into the computer systems of U.S. companies is at a record high this year and climbing."
- Numerous other sources are saying the same specifically about EHR breaches—just google "EHR breaches on the rise" (not in quotes).

Are EHRs Crucial to Providing Clients with the Best Possible Treatment?

Don't the best medical and psychological treatments both crucially depend on easy, *rapid* communication between these two professions? I don't see this, unless we're talking about certain types of integrated care settings such as pain or rehabilitation clinics, primary care centers, or medical specialty environments in which interprofessional teams work together and patients have multiple same-day appointments. (Whether these environments ought to have interoperable EHRs that make patient records available via the internet, or whether their electronic medical records should be limited to within-clinic computer systems, is an open question).

Outside of such settings, *rapid* accessibility of each other's diagnostic and treatment information by psychotherapists and physicians appears rarely useful. The discussion of the ER scenario above in the section on the 12/5/14 meeting addressed this question as well. Again, it makes little sense to risk the privacy of all psychotherapy clients for the benefit of a small fraction of ER patients, assuming this information would have any use at all in an ER.

Apart from rapid accessibility, do EHRs aid communication between professions? Surely they do. At the same time, are there easy work-arounds? Surely. For example, adults know their medical information and would also have access to it via their EHR portal. Clients can carry psychologist requests for specific medical assessments, for example related to anxiety disorders, by hand. If mailed, they would arrive long before a medical appointment occurred. The ease of communication via EHRs, a clear positive, does not appear in practice to buy us much when weighed against the risks.

Underlying this discussion is the fact that none of the psychotherapists I've interviewed on this subject who work outside of medical contexts have seen the need to interact with any client's physician more than exceedingly rarely.

What about communicating with a new client's last psychotherapist? I have never encountered a need to communicate *rapidly* with a past psychotherapist. And in these

cases, the phone may well be the best tool. Moreover, there are arguments on either side as to whether it is helpful to communicate at all with a past therapist about clients who are not significantly impaired.

At the bottom line, the risk to client privacy discussed above appears to greatly outweigh the convenience of having client information easily accessible on the internet.

The Unique Value of Smaller Psychotherapy Practices

We hear that smaller practitioners are being pushed out of the healthcare market. That larger entities will take over—behavioral health homes, accountable care organizations. And that small providers can now become part of a larger group—via EHRs.

But smaller settings have something unique to offer clients in the absence of EHRs: greater privacy as well as the greater feeling of privacy, which support effective psychotherapy. Larger settings may be fine for some, and the privacy of walking into a smaller clinic or private office is great for others. Strictly promoting one delivery model irresistibly recalls the wholesale loss of animal and plant species around the world. Every part of the ecosystem has a use and purpose and something of value to offer. Offering variety and choice reaches the greatest number of suffering human beings.

Unfairness to small practices. The EHR mandate would erode the added level of privacy that small providers are uniquely able to offer. Further, smaller, private providers who have practices of about five client hours per week (of whom I know several) would need to purchase: 1) internet service at their offices; 2) EHRs; 3) computers.

Summary

My purpose in writing is not to present a blanket argument against EHRs but rather against a *mandate* for their use with all psychotherapists and all clients. Internet security breaches are at an all time high and have been getting worse. Encrypted information is not always safe. EHRs aren't particularly useful to many psychotherapists or their clients relative to privacy threats to deeply personal information. Medical identity information is a prime target for theft. Minnesota is unique in mandating universal adoption of EHRs but is doing so on the basis of a law passed in 2007, well before the magnitude of data security threats and the costs associated with them were known. Our state is taking risks by sailing into uncharted waters regarding client privacy in service of an efficiency that has little value for many psychotherapists and their clientele.

Use of EHRs should be a clinical decision made between a client and psychotherapist after careful consideration of risks because it potentially affects the therapy itself. Psychotherapy requires not just privacy but the *feeling* of privacy, and evidence exists that EHR use inhibits disclosure. The security risks of EHRs may well turn out to be

unsolvable, in part because of the countless human beings, all of us imperfect, who would have potential access to a client's EHR. At this point in history, the internet shows no signs of becoming a place where security is assured. Clients and providers should be thoroughly conversant with the advantages of EHRs but have choice in whether to use them.

In writing to psychotherapists and other stakeholders, I am interested in eliciting other perspectives as well as feedback about anything I may have gotten wrong. But I am also interested in taking action to solve some of the problems associated with a blanket mandate.

Questions

Things we hear said among colleagues, in a statement like this one, at a seminar, or in informal conversation with MDH contacts may or may not be completely accurate. It's important to have answers to our questions in writing—that is, in a formal MDH document or in law. The following questions relate to various levels of safety for client privacy:

- Can psychotherapy notes be kept out of the EHR?
- Will MDH clarify the definition of "health care providers"—i.e. those to whom the mandate applies [see, "To Whom Does the Mandate Apply?"]? For example, does this definition allow exception for psychotherapists who do only fee-for-service work or who do only coaching or life enhancement work?
- Must a psychotherapist giving free services to a client record psychotherapy information about that contact on an EHR? [See "To Whom Does the Mandate Apply?"]
- If a client does not wish to have any information written on an EHR, does any law prohibit a provider from honoring this request?
- If a client refuses to have a psychotherapy EHR, would this mean the client couldn't have a medical EHR? [See "To Whom Does the Mandate Apply?"]
- At larger, multidisciplinary clinics, what alternatives to EHRs might exist that would have the efficiency and convenience of EHRs without as much risk?
- Is there anything in law or ethics prohibiting a therapist from refusing to see clients who request an EHR (say, owing to privacy concerns—i.e., reasonably founded concerns that doing so could harm the client) and referring them elsewhere?
- If psychotherapists do not see clients who request EHRs or if all their clients refuse EHRs, and if none of this violates any law or rule, do psychotherapists still need to buy and somehow use an EHR? (I raise this odd question because the answer was "yes" at the 11/20/14 seminar. On the other hand, in a 10.31.14 phone conversation, an MDH contact stated "probably not" and that MDH probably recommends "going with whoever is the governing entity for your health care type.")

- Is a scalable solution possible—a mandate that might apply to larger clinics but not smaller providers?

Possible Next Steps

As stated in the cover email, there appear to be at least three general areas of hope:

- Can the Minnesota Department of Health support an interpretation of law that allows some psychotherapists and their clients choice in whether to use EHRs or not?
- Can the law itself be changed to allow the same?
- Can the law be successfully challenged?

Do enough people have the energy and motivation to work for change? Many hands make light work. Will several people lead? Can we create cells of activity? The following is a rough sketch of possible steps. Different people could:

- Find a way to get this document to other psychotherapist groups.
- Work with MDH to get answers to questions such as those in the last section.
- Create an email campaign or petition to the Commissioner of Health, Edward Ehlinger, MD, before his annual report is issued next month (https://www.revisor.mn.gov/statutes/?id=62j.495 subd. 2 (4)(c))?
- Conduct email or petition campaigns to legislators? To others?
- Produce a newsletter to announce email campaigns, progress, etc.
- Work with the Board of Psychology—will the board, whose mission is to protect the public, interest itself in these issues?
- Learn and inform us of political strategies for changing the law.
- Create or sit on committees in our professional organizations, leading for example to lobbying.
- Write letters to the editor.
- Determine whether other professional groups will join us (a Rand study showed mixed reactions to EHRs among physicians-- http://www.rand.org/pubs/research_reports/RR439.html . . .would many support choice over mandate?).
- Determine whether a group like the ACLU would be interested in our issues with EHRs and privacy. "The ACLU's Project on Speech, Privacy, and Technology monitors the interplay between cutting-edge technology and civil liberties, actively promoting responsible uses of technology that enhance privacy protection, while opposing those that undermine our freedoms and move us closer to a surveillance society" (https://www.aclu.org/technology-and-liberty). Indeed, are there federal laws that this mandate, unique among the fifty states, violates?
- Plan and determine overall strategy, order of steps, and suggest other steps.

What I'll do. I hope this long work has provided a foundation from which to begin, if you happen to be interested. Are you? For a variety of personal reasons, I won't take a leadership role, but I'll serve. For example, this document has reached a few thousand licensed psychologists in Minnesota. Will you send me back an email if you're willing to work on any of the steps above or other steps you've thought of? If it's only participating in email or petition campaigns, that's still a significant contribution—numbers will be important. I'll collect email addresses of those interested in participating in given activities and circulate them to others with the same interests in early January.

Can we be like a human organism constructing itself? Identical cells spontaneously differentiate themselves into different needed parts, then work together. Important for working together would be a committee to handle a newsletter. Knowing what others are doing is greatly motivating as is knowing there are lots of us, if that happens to be the case. Can we do this? To me, the alternative is the Apple 1984 advertisement (https://www.youtube.com/watch?v=VtvjbmoDx-I). Instead, we could accomplish a very good thing for psychotherapy in Minnesota.

Whatever, in connection with my professional practice or not in connection with it, I see or hear in the life of men, which ought not to be spoken of abroad, I will not divulge, as reckoning that all such should be kept secret.

—from the Hippocratic Oath